

What Is Identity Fraud and Theft?

- Identity Fraud and Theft involves all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.
- Fraud is an intentional perversion of the truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender some legal right.

What is Identity Fraud? §16-13-510

- > Without the authorization or permission of another person With the intent of unlawfully appropriating the financial
- To his/her own use or
- resources of that person To the use of a third party
 - Obtains or records identifying information which would assist in accessing the financial records or
 - Accesses or attempts to access the financial resources of the other person through the use of identifying information
 - Examples: SSN, Driver's License #, Checking Account #, Credit Card #, digital signatures, etc.

What is Identity Theft?

- Financial Transaction Card Theft
 - > § 16-14-20: Obtains FTC from another without the cardholder's consent and with the intent to use it, sell it or transfer it to a person other than the issuer or cardholder
- **Financial Transaction Card Forgery**
- § 16-14-40
- **Financial Transaction Card Fraud**
 - ≽ § 16-14-40
- **Criminal Possession of Financial Transaction Card Forgery**
 - > §16-14-70

Why Worry About Identity Fraud and Theft?

- It is the fastest-growing crime in the nation.
- More than 10 million people are victimized by it each year. The most victimized group being those between the ages of 19 and 29.
- It can cost an average of 80 hours and more than \$1,400 to clear up a simple case of identity theft that is caught early.
- Some victims lose many thousands of dollars as well as their good credit rating and consumer reputations.
- It costs our economy \$40 billion or more each

Why Worry About Identity Fraud and Theft? (cont.)

- Prevention is the best defense.
- There are jurisdictional problems concerning where the crime occurs.
- It is an attractive crime to criminals because of its low risk and high return.

How Identity Fraud and Theft Works STEP 1—Getting the Identity "Wholesale" – when someone obtains lists of information on individuals through computer hacking, theft, or bribery. "Shoulder Surfing" – when someone watches you from a nearby location as you punch in your telephone calling card number or credit card number or pin number. "Dumpster Diving" – when someone goes through your trash to obtain copies of your checks, credit card or bank statements or other records that bear your name, address and telephone numbers. "Phishing" – Illegitimate emails or pop-up messages posing as your bank, credit card or utility company.

How Identity Fraud and Theft Works STEP 1 – Getting the Identity (cont.) Pre-approved Credit Card Applications – when someone retrieves them and activates a card for their use without your knowledge. Unsolicited E-mails – emails that promise benefits but request identifying information Telephone calls asking you to "update records" Second Impressions of credit cards Theft of incoming bills, which show your account number Theft of outgoing mail and bill payments

How Identity Fraud and Theft Works STEP 2—Exploiting the Identity The thief may have false IDs made in order to begin leveraging one piece of information to obtain or establish other information or assets. These may include New credit card accounts State or local licenses Accounts with utility companies, apartment leases, or even home mortgages.

Who Is Vulnerable? (cont.) People who Don't regularly check their credit bureau reports Have accessible mail boxes

People who Keep their money in bank accounts Use credit or debit cards Generate trash with unshredded paper in it Casually toss credit card or other receipts into public receptacles Get personal bills by mail or electronically Don't check their credit card reports and bank statements

Prevention "S" - Be STINGY about giving out your personal information "C" - CHECK your financial information regularly "A" - ASK periodically for a copy of your credit report "M" - MAINTAIN careful records of your banking and financial accounts for at least 1 year

Prevention (cont.)

- Register with the Direct Marketing Association to stop unsolicited credit offers.
- Deposit mail in a U.S. Postal Service Mail Box.
- Secure your mailbox or get a P.O. Box for your bills.
- Call your bank or credit card company immediately if you do not receive your bill.

Reporting and Restoring

- Contact their local police agency first and foremost. The victim <u>needs</u> to file a report.
- Call your financial agencies and put a fraud alert on your accounts.
- Contact their local FBI Office or U.S. Secret Service Office.
- Contact the Federal Trade Commission (FTC) to report the situation at 1-877-ID THEFT of www.ftc.gov.

Reporting and Restoring (cont.)

- Contact the fraud units of the 3 principle credit reporting companies:
 - Equifax at 1-800-525-6285
- Experian at 1-888-397-3742
- > Trans Union at 1-800-680-7289
- The victim <u>mav</u> need to consult with a civil attorney for necessary, specific steps in a given state.
- Check court records in your general area for bankruptcies and for mortgage liens using your name. Many records are automated, which makes the job easier.

Reporting and Restoring (cont.)

- Obtain copies of all records which show the fraudulent activity.
- Get counseling if needed.

Online Resources

- Federal Trade Commission: www.ftc.gov
- Department of Justice:
 - www.usdoj.gov/criminal/fraud/idtheft.html
- > Better Business Bureau: www.bbb.org
- ➤ United States Postal Services: www.usps.com

Online Resources (cont.)

- Many nonprofit organizations are committed to promoting prevention and recovery from identify theft. Here are a few:
- www.idtheftcenter.com/index.shtml
- www.identitytheft.org/
- www.privacyrights.org/identity.htm